In re Patent Application of
MACCHETTI ET AL.
Serial No. **09/974,705**
Filed: **OCTOBER 10, 2001**

In the Claims:

This listing of claims replaces all prior versions and listing of claims in the application.

Claims 1-20 (canceled).

21. (Currently amended) A method of converting data between an unencrypted format and an encrypted format, the data being organized in bit words, the method comprising:

performing a plurality of transformation rounds~~, each transformation round~~ comprising

applying at least one transformation to a two-dimensional array of rows and columns of bit words defining a state array; and

~~transposing~~ exchanging each of the rows ~~and~~ with a respective column ~~columns~~ of the state array to form a transposed state array for at least one of the transformation rounds so that the at least one transformation is applied to the transposed state array.

22. (Previously presented) A method according to Claim 21 wherein the bit words are 8-bit words.

23. (Previously presented) A method according to Claim 21 wherein the state array is a 4 x 4 matrix of bit words.

24. (Previously presented) A method according to Claim 21 wherein the plurality of transformation rounds comprises at least 10 transformation rounds.

25. (Currently amended) A method according to Claim 21 wherein performing further comprises ~~determining a non-transposed state array in at least one of the plurality of transformation rounds, and~~ performing at least one transformation round ~~once the~~ on a non-transposed state array ~~in at least one of the plurality of transformation rounds occurs~~.

26. (Previously presented) A method according to Claim 21 further comprising applying at least one round key to the state array in at least one of the transformation rounds.

27. (Previously presented) A method according to Claim 26 wherein the at least one round key is transposed before being applied to the state array.

28. (Previously presented) A method according to Claim 26 further comprising adding code to transpose the at least one round key.

29. (Previously presented) A method according to Claim 26 wherein the at least one round key comprises a plurality of round keys, each corresponding to a respective transformation round and being applied according to a round key schedule.

30. (Previously presented) A method according to Claim 29 wherein the round key schedule comprises a transposed round key schedule.

31. (Currently amended) A device for converting data between an unencrypted format and an encrypted format, the device comprising:

at least one register for storing the data in the form of bit words; and

a circuit for

performing a plurality of transformation rounds, each transformation round comprising applying at least one transformation to a two-dimensional array of rows and columns of bit words defining a state array, and

~~transposing~~ exchanging each of the rows ~~and~~ with a respective column ~~columns~~ of the state array to form a transposed state array for at least one of the transformation rounds so that at least one transformation is applied to the transposed state array.

32. (Previously presented) A device according to Claim 31 wherein said at least one register stores bit words as 8-bit words.

33. (Previously presented) A device according to Claim 31 wherein said circuit operates on a state array comprising a 4x4 matrix of bit words.

34. (Previously presented) A device according to Claim 31 said circuit in performing a plurality of transformation rounds performs at least 10 transformation rounds.

35. (Previously presented) A device according to Claim 31 wherein said circuit comprises at least one S-box processing module, said at least one S-box processing module operating on a group of bit words defining a cell of a column of the state array.

36. (Previously presented) A device according to Claim 35 wherein the at least one S-box processing module comprises a plurality of S-box modules, each of the plurality of S-box modules operating on a corresponding cell of a column of the state array.

37. (Previously presented) A device according to Claim 36 wherein the column of the state array comprises four cells.

38. (Previously presented) A device according to Claim 31 wherein the circuit further comprises a plurality of shift column modules, each of said plurality of shift column modules to perform a column shift operation on a column of the state array.

39. (Previously presented) A device according to Claim 38 wherein a column shift operation performed by each of said plurality of shift column modules generates shift column

data, and wherein said circuit further comprises a single mix column module to perform column mix operations on shift column data.

40. (Previously presented) A device according to Claim 31 wherein said circuit is an encoder for converting data from an unencrypted data format to an encrypted data format.

41. (Previously presented) A device according to Claim 40 wherein said circuit is an embedded system for use in a smart card.

42. (Previously presented) A device according to Claim 31 wherein said circuit is a decoder for converting data from an encrypted data format to an unencrypted data format.

43. (Previously presented) A device according to Claim 42 wherein said circuit is an embedded system for use in a smart card.

44. (Currently amended) A device for converting data between an unencrypted format and an encrypted format, the device comprising:

at least one register for storing the data in the form of bit words; and

a circuit for

performing a plurality of transformation rounds, each transformation round comprising applying at least one transformation to a two-

dimensional array of rows and columns of bit words defining a state array,

~~transposing~~ exchanging each of the rows ~~and~~ with a respective column ~~columns~~ of the state array to form a transposed state array for at least one of the transformation rounds so that at least one transformation is applied to the transposed state array, and

applying at least one round key to the state array in at least one of the transformation rounds.

45. (Previously presented) A device according to Claim 44 wherein said circuit comprises a plurality of S-box modules, each of the plurality of S-box modules operating on a respective group of bit words, each group defining a cell of a column of the state array.

46. (Previously presented) A device according to Claim 45 wherein the circuit further comprises a plurality of shift column modules, each of said plurality of shift column modules to perform a column shift operation on a column of the state array.

47. (Previously presented) A device according to Claim 46 wherein a column shift operation performed by each of said plurality of shift column modules generates shift column data, and wherein said circuit further comprises a single mix column module to perform column mix operations on shift column data.